

Donnelley Financial Solutions

Information Security Policy (extract)

Internal Use Only

Revision History

Version	Date	Author	Description
1.0	01/08/2016	IT Governance	Annual Review – no updates
2.0	03/02/2017	DFS IT Governance	2017 Annual review - Minor updates to Password Policy section
3.0	06/25/2018	IT Security, Governance & Privacy	2018 Annual Review
3.1	07/15/2018	IT Security, Governance & Privacy	Reviewed with Security updated section 8.1.4
4.0	09/19/2019	IT Security, Governance & Privacy	Reviewed and strengthen areas with Security, Privacy and Governance
5.0	08/20/2020	IT Security and Governance	Reviewed. Minor updates.
6.0	8/30/2021	Governance	Reviewed. Minor updates

Approval



9/3/2021

Dannie Combs, SVP - Chief Information Security Officer

1.0 INTRODUCTION

Objective

Donnelley Financial Solutions Information Security Program is designed to ensure the proper level of security throughout the environment. The Information Security Program is based on business requirements derived from:

1. Assessing security risks to the organization.
2. Defining the legal, statutory, regulatory, and contractual requirements that Donnelley Financial Solutions, our business partners, contractors, and service providers have to satisfy.
3. Delineate the principles and objectives for operational information processing.

Information Security is achieved by implementing a set of controls, which consist of policies, processes, procedures, organizational structures, and software functions. These controls need to be established to minimize risk and protect information assets that are required by Donnelley Financial Solutions to meet the operational, financial, and regulatory requirements of its businesses. Information security is characterized as the preservation of Availability, Integrity and Confidentiality.

Availability – Prevents disruption of service and productivity

Integrity – Prevents unauthorized modification of systems and information

Confidentiality – Prevents unauthorized disclosure of sensitive information

1.1 Information Security Policy

This Information Security Policy comprises various sections, which outline the Donnelley Financial Solutions Information Security Policies. These policies establish the rules for implementing a comprehensive Information Security program.

Audience

The information security policies outlined in this manual apply to all employees, consultants, temporary personnel, or others who have access to Donnelley Financial Solutions information, each of which have an obligation to protect it from unauthorized access, modification, disclosure, and destruction, whether accidental or intentional in nature.

Monitoring and Enforcement

All activities on Donnelley Financial Solutions information assets are subject to logging and review. In addition to regular internal audits, information assets are subject to being monitored for security policy compliance. Violations of standards, procedures, or established in support of this policy manual shall be brought to the attention of management for appropriate action and referred to the Human Resource and or Legal Department.

3.0 ACCEPTABLE AND ELECTRONIC USE

Objective

This section establishes the rules of conduct for Donnelley Financial Solutions employees and contractors in the use of Donnelley Financial Solutions information systems and the handling of private or confidential data or documents.

3.1 Expectation of Privacy/Right to Monitor

Donnelley Financial Solutions may log, review, and otherwise utilize any information stored on or passing through its information systems for the purpose of managing and enforcing the security of our network infrastructure to protect company, employee, and customers' data. For these same purposes, Donnelley Financial Solutions may also capture user activity such as telephone numbers dialed, and web sites visited.

Donnelley Financial Solutions management reserves the right to examine electronic mail messages, files on company-issued computers, web browser cache files, web browser bookmarks, logs of web sites visited, and other information stored on or passing through Donnelley Financial Solutions computers. Such management access assures compliance with internal policies, assists with internal investigations, and assists with the management of Donnelley Financial Solutions information systems.

A wide variety of business partners have entrusted their information to Donnelley Financial Solutions for business purposes, and all personnel employed by Donnelley Financial Solutions must do their best to safeguard the privacy and security of this information. The most important of these business partners is the individual customer; customer account data is accordingly confidential, and access will be limited based on business need for access. You may read more about our privacy practices by visiting. <https://www.dfinsolutions.com/privacy-notice>

3.2 Electronic Communications Privacy

Definitions:

Electronic Communications System - refers to all computers, computer systems, voicemail, electronic messaging systems or services, document collaboration system or services, online application services, network, intranet, or internet access system owned, leased, contracted, operated, maintained, or managed by Donnelley Financial Solutions.

Donnelley Financial Solutions reserves the right to monitor, access, retrieve and read all messages and content, and to disclose any message to law enforcement officials or other third parties, without any prior notice to the originator or recipient of the message. Additionally, supervisors and managers may review messages to and from employees they supervise or manage. Employees should have no expectation of privacy regarding anything sent, posted, received, or accessed through the Electronic Communications System.

Messages may not contain content that may be considered offensive, disruptive, defamatory, or derogatory, including but not limited to sexual comments or images, racial slurs, or other comments or images that would offend someone based on his or her race, national origin, gender, sexual orientation, religious, or political beliefs or disability. Users may not transmit copyrighted materials, trade secrets, and confidential or proprietary information without proper authorization. Where possible, the transmission of sensitive and confidential data should be authenticated using digital signatures or encrypted in accordance with Donnelley Financial Solutions encryption specifications.

Employees may not use the organization's systems to access, download, or transmit material which is inappropriate, offensive, illegal, or which degrade existing security controls. Confidential or private information should not be recorded unless authorized. All parties must be notified in advance whenever conversations are being recorded.

3.3 Remote Access of a Workstation

Users are not permitted to install software to allow remote control of a Donnelley Financial Solutions workstation. Remote control of a Donnelley Financial Solutions workstation is only permitted by appropriate systems support personnel using methods of remote control approved by Governance, Risk and Compliance and Security. Users may use “desktop” sharing features of software or other web conferencing tools.

However, users may not permit others to “take control” of their workstation through such applications, unless it is in the context of receiving support, during a presentation, demo, or training from appropriate systems support personnel. Use of desktop sharing capabilities are not permitted when a workstation is unattended. Users are not permitted to use software to remotely access or control non-Donnelley Financial Solutions computers, unless it is for appropriate Donnelley Financial Solutions business purposes.

3.3.1 Working from an Alternative Location

Offsite computer usage, whether at home or at other locations, should only be conducted with authorization by a user’s management. Usage should be restricted to business purposes, and users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures. Whether employees are in the office or at an alternate work site, all intellectual property developed or conceived of while an employee is attending to Donnelley Financial Solutions business is the exclusive property of Donnelley Financial Solutions. Such intellectual property includes patent, copyright, trademark, as well as all other

intellectual property rights as manifested in memos, plans, strategies, products, computer programs, documentation, and other materials and this property must be protected according to this security policy manual.

Confidential or private information is not to be transmitted to an offsite location, except in a manner consistent with sections 2.4 Removable Media and 3.3.3 Securing Information on Mobile Devices. Employees attending to business at alternative work sites should only use Donnelley Financial Solutions provided computer software, hardware, and network equipment. When Donnelley Financial Solutions supplies an employee with software, hardware, information, data or other materials to perform business remotely, the title to, and all rights and interests to these items, shall remain with Donnelley Financial Solutions. In such instances, employee possession does not convey ownership or any implication of ownership. Accordingly, all such items must be promptly returned when an employee separates from Donnelley Financial Solutions.

3.3.2 Remote Access

Remote access to the Donnelley Financial Solutions network is only permitted from Donnelley Financial Solutions owned or issued equipment (where applicable). Access from equipment not owned or issued by Donnelley Financial Solutions is prohibited without an approved exception. Remote access to the Donnelley Financial Solutions network and resources will only be permitted where authorized users are authenticated, data is encrypted across the network and privileges are restricted. All remote access to Donnelley Financial Solutions information assets will be accomplished utilizing DFIN provided VPN solution with two factor authentications and/or stronger. All other external facing applications will require appropriate login methods with security appropriate to the content within the application.

3.3.3 Securing Information on Mobile Devices

Donnelley Financial Solutions confidential or private information must not be stored on mobile computing devices. Temporary storage of information for work in progress is acceptable; however, the information must be copied to a network file server and removed from the mobile computing device as soon as practical. Where confidential or private information must be stored on a mobile device, the manner in which it is stored and then destroyed must follow the guidelines established in sections 2.4 Removable Media and 2.5 Disposal of Electronic Storage Media on the use of removable media. As such, information classified as confidential or private must be encrypted when it is stored on mobile computing devices.

3.3.4 Mobile Employee Responsibilities

Users are responsible for the security of information in their custody, to include mobile devices. Users must not leave mobile devices unattended. Users must refrain from conducting business when connected to a public wireless hotspot or other public network unless they are utilizing the standard Donnelley Financial Solutions remote access VPN service.

Personnel accessing cardholder data via remote access technology are prohibited from copying, moving or storing cardholder data to removable media or local hard drives unless required for a specific authorized business need. Users must not share dynamic password token cards, smart cards, fixed passwords, or any other access devices or access parameters with any other person without prior approval from Security and Governance, Risk and Compliance and Security. Family members, friends, or others must not be permitted to use the assigned equipment. Users must promptly report to their manager and to the IT Help Desk any damage to or loss of computer hardware, software, or confidential or private information that has been entrusted to their care.

3.4 Acceptable Use Policy

This section depicts the behaviours that are considered acceptable in the Donnelley Financial Solutions environment.

Donnelley Financial Solutions electronic communications system is intended to facilitate company business. Therefore, primary usage of this system should be limited to business related purposes. Incidental personal use of Donnelley Financial Solutions electronic communication system is permitted but should be kept to a minimum using language and standards consistent with other forms of business communication.

3.4.1 General Use and Ownership

All employees must be aware that the data they create on any corporate systems remains the property of Donnelley Financial Solutions. Users must consider the sensitivity level of the information in which they handle and properly apply the appropriate protection level based on the Information Classification and Handling policies defined elsewhere in policy. Employees are responsible for notifying the appropriate manager if they have access to confidential information for which they do not have a business requirement.

3.4.2 User Password and Account Management

Users are responsible for all activities performed with their assigned IDs. IDs may not be utilized by anyone but the individual to whom they have been issued. Authorized users are responsible for the security of their passwords and accounts. Passwords must be treated as confidential information. Passwords must not be easy to guess and must not be recorded or stored on paper or electronically in clear text. Users must not divulge their passwords for any reason this includes system administrators.

If the confidentiality of a password is in doubt, the password must be changed immediately. System administrators must not circumvent the Password Policy for the sake of ease of use. Users must not circumvent user interactive password entry with auto logon, application remembering, embedded scripts, or hard coded passwords in client software. PCs, laptops and workstations must be secured with a password protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging off when the computer will be unattended. Users must not disable or alter the screensaver or change the password protection setting. Any changes to policy, require an approved exception.

3.4.3 User Network Access

Connections to the Donnelley Financial Solutions network, either onsite or remotely, are permitted only for Donnelley Financial Solutions owned assets. The connection of non-Donnelley Financial Solutions assets is not permitted unless approval has been granted by Security, Governance Risk and Compliance, and/or business unit, or if it is to an isolated network segment designed for connection by customers of Donnelley Financial Solutions or visitors to Donnelley Financial Solutions facilities.

Users must not establish any communications system that accepts incoming dial-up calls or bridges network connections into the Donnelley Financial Solutions network. Users may not connect wireless access points to the Donnelley Financial Solutions network unless they are approved by IT Network Engineering and compliant with applicable wireless device security configuration standards.

3.4.4 Malicious Code Prevention

Computers connected to the Donnelley Financial Solutions network must continually run approved antivirus software with a current virus database. Frequency of the virus database updates is determined by standard. Users must not disable the installed antivirus software or other information security applications or interfere with their scheduled scans or updates. Users should contact the Help Desk if their antivirus software reports that their computer has been infected.

3.4.5 Remote Access of a Workstation

Users are not permitted to install software to allow remote control of a Donnelley Financial Solutions workstation. Remote control of a Donnelley Financial Solutions workstation is only permitted by appropriate systems support personnel using methods of remote control approved by Governance, Risk and Compliance and Security. Users may use "desktop" sharing features of software or other web conferencing tools. However, users may not permit others to "take control" of their workstation through such applications, unless it is in the context of receiving support, during a presentation, demo, or training from appropriate systems support personnel. Use of desktop sharing capabilities are not permitted when a workstation is unattended. Users are not permitted to use software to remotely access or control non-Donnelley Financial Solutions computers, unless it is for appropriate Donnelley Financial Solutions business purposes

3.4.6 Security of Electronic Email

Email should only be used for business purposes, using terms which are consistent with other forms of business communication. Users must ensure that information forwarded by (especially attachments) is correctly addressed and sent only to appropriate persons. Customer owned data may not be transmitted via email in any manner without customer authorization or refer to a contract that has been agreed upon. If allowed by contract, sending data externally should be the contractual provisions agreed to or if not proscribed then by most secure method available, but never in plain text or over unsecured network.

Private or confidential information should not be transmitted as text in the body of an email. Where it is necessary to transmit private or confidential information by email, the information should be sent as an encrypted attachment, and sent to only those who have a business requirement to handle that specific information. Email addresses should be verified before sending attachments with confidential or private information. The attachment of data files to email is only permitted after confirming the classification of the information being sent. Users are responsible for ensuring attachments are free of viruses, malware, or other malicious code.

Users should treat unsolicited emails with caution and should use caution following email best practices and electronic communication. Internal phishing exercises are performed within the DFIN environment regularly to ensure proper security measures are being taken by the end user.

Similar with all other Donnelley Financial Solutions' electronic communication systems, use of electronic email for incidental personal use is permitted but should be kept to a minimum and must use language and standards consistent with other forms of business communication. The use of third-party Personal Email addresses (Gmail, Yahoo, Hotmail) for business purposes is only permitted by approval from senior management. Also, see section 3.2 Electronic Communications Privacy, 3.3.3 Securing Information on Mobile Devices, and 3.3.4 Mobile Employee Responsibilities

3.4.7 Security of Electronic Office Systems

Employees must prove the identity of the person on the telephone before communicating confidential or private information. Employees must shred faxes that contain sensitive or confidential information that are received in error. Employees must only fax sensitive or confidential information when secure methods of transmission are not possible. Both the sender and the receiver must agree to the transmission of the information. Employees must verify fax numbers before sending confidential or private information.

3.4.8 Allowed Security Services

Employees may only access websites through standard Donnelley Financial Solutions security services (for example firewalls, approved URL filters). Employees may not bypass Donnelley Financial Solutions security services by any means, including configuring their workstations to use alternative and or proxy servers. Workstations configured to use specific Donnelley Financial Solutions security services may not be reconfigured by employees to use alternative services without prior authorization from Governance Risk and Compliance and Security.

3.5 Clean Desk and Clear Screen

Employees must keep their work area clean and orderly. Confidential and private information must not be left unattended on desks, screens, printers or any other media including conference room whiteboards. Employees must organize and file information based on the classification level of the information. Approved login procedures must be strictly observed and users leaving their screen unattended must firstly lock access to their workstation or log off. The display screens for all systems used to handle confidential or private information must be positioned so that unauthorized persons cannot readily view them through a window, over the shoulder or by similar means.

Donnelley Financial Solutions confidential and private information must only be generated in hard copy to the extent necessary to complete normal business operations. Confidential and private information must not be left unattended when it is printed, faxed, and/or copied and must be secured when not in use. All confidential or private

information on hard copy (paper) must be destroyed by shredded before disposal. Intermediate work products related to confidential or private information, such as carbon copies or memo drafts, must also be shredded when final work product is produced.

3.6 Reporting Suspicious Activities or Security Incidents

Users must promptly report to their manager and to the IT Help Desk (The care Center) any damage to or loss of computer hardware, software, or confidential or private information that has been entrusted to their care. This includes reporting the theft of users' laptop computers to your immediate manager, opening an incident ticket with the help desk and requires a police report. Users must report any activity by staff, consultants, contractors or guests that may result in the disclosure or destruction of Donnelley Financial Solutions or customer information assets.

Listed below are common activities that should be reported:

1. Recording customer data to removable media when not required by the business process.
2. Using cameras or cell phones equipped with cameras in areas where customer data is being processed.
3. Allowing unauthorized personnel into restricted areas.

In addition to these, any activity that an employee believes could have a negative impact on Donnelley Financial Solutions information to include customer data, must be reported.

3.7 Unacceptable Use

This section depicts the behaviours that are considered unacceptable in the Donnelley Financial Solutions environment. Employees may not use anonymizer services or peer-to-peer software (e.g. Tor or other tools).

3.7.1 Unauthorized Activities

Under no circumstances is an employee of Donnelley Financial Solutions authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Donnelley Financial Solutions resources. **A Donnelley Financial Solutions employee must not violate the intellectual or property rights of any person or company such as copyrights, patents, code, or trade secrets.** Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal and not acceptable behaviour. The appropriate legal counsel must be consulted prior to export of any material that is in question.

3.7.2 Unauthorized Usage

Users must not attempt to access any data or programs contained on Donnelley Financial Solutions systems for which they do not have authorization or explicit consent. Users must not leave messages that contain sensitive or confidential information on answering machines or voicemail systems. Users must not disclose sensitive or confidential information in public places when using mobile or public phones.

Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any Donnelley Financial Solutions computer system. Externally supplied floppy disks, CD-ROMs, and other removable storage media must not be used unless authorized and have been checked for viruses. Attachments to electronic mail must not be executed or opened unless they have been checked for viruses.

3.7.3 Unacceptable Network Activities

- Install network hardware or software that provides network services without approval from appropriate IT Network Engineering.
- Attempt to interrogate or map the networks of other companies or organizations.
- Divulge dial up or dial back modem phone numbers to unauthorized users.
- Alter Donnelley Financial Solutions supplied information assets hardware in any manner.
- Attach non-DFIN device to DFIN network

- Extend or retransmit network services in any way. For example, users must not install a modem, router, switch, hub, or wireless access point on the network, or enable software proxy services without IT Network Operations approval.
- Modify IP addresses or network configuration settings or add, remove or modify hardware or software on their Donnelley Financial Solutions computer system.

3.7.4 Unacceptable Email Activities

Users must not use electronic communication systems for purposes of political lobbying or commercial unless explicitly approved by Donnelley Financial Solutions management. Users should be aware of the inherent risks of all incoming email and should not respond to unsolicited email or open file attachments unless they have been scanned for possible viruses or malicious code. Users should not attach data files to email without considering the sensitivity of the information being sent and assuring that the file does not contain viruses or other malicious code. Users may not forge or attempt to forge email messages, or disguise or attempt to disguise their identity when sending email.

Users must not participate in the interception, eavesdropping, recording or altering another person's email messages or adopt the identity of another person in any message. Users must not send messages that may be construed as a threat or related to acts or instruments of violence. Users must only send Donnelley Financial Solutions data, business partner data to authorized persons who have a need to know. Users must not use "texting" for business purposes.